


Ex. D - Claim Chart

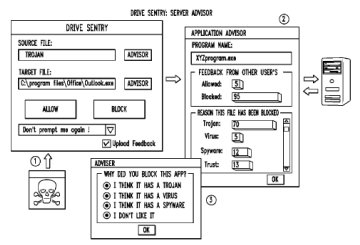
U.S. Patent No. 7,664,924



US007664924B2

<p>(12) United States Patent Safa</p> <p>(54) SYSTEM AND METHOD TO SECURE A COMPUTER SYSTEM BY SELECTIVE CONTROL OF WRITE ACCESS TO A DATA STORAGE MEDIUM</p> <p>(75) Inventor: John Safa, Park Estate (GB)</p> <p>(73) Assignee: Drive Sentry, Inc., Mountain View, CA (US)</p> <p>(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.</p> <p>(21) Appl. No.: 11/858,752</p> <p>(22) Filed: Sep. 20, 2007</p> <p>(65) Prior Publication Data US 2008/0114957 A1 May 15, 2008</p> <p>Related U.S. Application Data</p> <p>(63) Continuation-in-part of application No. 11/292,910, filed on Dec. 1, 2005.</p> <p>(60) Provisional application No. 60/826,377, filed on Sep. 20, 2006.</p> <p>(51) Int. Cl. G06F 12/14 (2006.01)</p> <p>(52) U.S. Cl. 711/163; 711/E12.091; 711/E12.093; 711/E12.096</p> <p>(58) Field of Classification Search 711/163 See application file for complete search history.</p> <p>(56) References Cited U.S. PATENT DOCUMENTS 5,410,700 A 4/1995 Fecteau et al. 5,778,432 A * 7/1998 Rubin et al. 711/135 5,825,877 A 10/1998 Dan et al. 5,974,549 A * 10/1999 Golan 726/23</p>	<p>(10) Patent No.: US 7,664,924 B2</p> <p>(45) Date of Patent: Feb. 16, 2010</p> <p>5,991,777 A * 11/1999 Momoh et al. 707/205</p> <p>(Continued)</p> <p>FOREIGN PATENT DOCUMENTS GB 2402515 B1 12/2004</p> <p>(Continued)</p> <p>OTHER PUBLICATIONS Norton Internet Security 2000. Manual [online]. Symantec Corporation, 1999 [retrieved on Jan. 29, 2008]. Retrieved from the Internet: <URL: http://webpages.charter.net/cw/mis/pdf/*></p> <p>(Continued)</p> <p>Primary Examiner—Reginald G. Bragdon Assistant Examiner—Larry T. Mackall (74) Attorney, Agent, or Firm—Ted Sabety; Sabety +associates, PLLC</p> <p>(57) ABSTRACT A system and method to securing a computer system from software viruses and other malicious code by intercepting attempts by the malicious code to write data to a storage medium. The invention intercepts the write access requests made by programs and verifies that the program is authorized to write before letting the write proceed. Authorization is determined by using the identity of the program as a query element into a database where permission values are stored. Depending on the presence or value of the permission value, write access is permitted or denied. Permission values can be set by the user, downloaded from a central server, or loaded into the central server by a group of users in order to collectively determine a permission value. The interception code can operate in kernel mode.</p>
---	---

11 Claims, 8 Drawing Sheets



Ex. D – Claim Chart
U.S. Patent No. 7,664,924

CLAIM 1	SOPHOS PRODUCTS
<p>1[pre] In a computer comprising a storage medium and an application running on said computer, a method of controlling write access to said storage medium by said application comprising:</p>	<p>Sophos offers various software that performs the method of claim 1. Specifically, Sophos offers many applications to protect against electronic threats such as viruses, ransomware, malware, and the like. That software includes features such as Sophos Anti-Virus, Sophos Behavior Monitoring, and/or Sophos Live Protection. For example, the infringing products that incorporate those features include Endpoint Security and Control, Central Endpoint Protection, Intercept X, Intercept X Advanced, Intercept X Advanced with EDR, Home, and Home Premium.</p> <div style="border: 1px solid black; padding: 5px; margin: 10px 0;"> <p>Sophos Endpoint Security and Control is an integrated suite of security software.</p> <p>Sophos Anti-Virus detects and cleans up viruses, Trojans, worms, and spyware, as well as adware and other potentially unwanted applications. Our HIPS (Host Intrusion Prevention System) technology can also protect your computer from suspicious files and rootkits. In addition, Malicious Traffic Detector can detect communications between your computer and command and control servers involved in a botnet or other malware attack.</p> <p>Sophos Behavior Monitoring uses our HIPS technology to protect Windows computers from unidentified or "zero-day" threats and suspicious behavior.</p> <p>Sophos Live Protection improves detection of new malware without the risk of unwanted detections. This is achieved by doing an instant lookup against the very latest known malware. When new malware is identified, Sophos can send out updates within seconds.</p> <p>Sophos Web Protection provides enhanced protection against web threats by preventing access to locations that are known to host malware. It blocks endpoints' access to such sites by performing a real-time lookup against Sophos's online database of malicious websites. It also scans downloaded data and files and checks file reputation.</p> <p>Sophos Application Control blocks unauthorized applications such as Voice over IP, instant messaging, file sharing, and game software.</p> <p>Sophos Device Control blocks unauthorized external storage devices and wireless connection technologies.</p> <p>Sophos Data Control prevents the accidental leakage of personally-identifiable information from managed computers.</p> <p>Sophos Web Control provides protection, control, and reporting for computers that are located, or roam, outside the corporate network.</p> <p>Sophos Client Firewall prevents worms, Trojans, and spyware from stealing and distributing sensitive information, and also prevents intrusion from hackers.</p> <p>Sophos AutoUpdate offers fail-safe updating and can throttle bandwidth when updating over low-speed network connections.</p> <p>Sophos Tamper Protection prevents unauthorized users (users with limited technical knowledge) and known malware from uninstalling Sophos security software or disabling it through the Sophos Endpoint Security and Control interface.</p> </div> <p>https://docs.sophos.com/esg/endpoint-security-and-control/10-6/help/en-us/PDF/sesc_h.pdf at 2</p>

Ex. D – Claim Chart
U.S. Patent No. 7,664,924

CLAIM 1	SOPHOS PRODUCTS																																																																																																																																						
1[pre] In a computer comprising a storage medium and an application running on said computer, a method of controlling write access to said storage medium by said application comprising:	<p>Relevant features discussed in this chart span the software of Endpoint Security and Control, Intercept X, Intercept X Advanced, Intercept X Advanced with EDR, Central Endpoint, Home, and Home Premium as shown in this charts. Upon information and belief, Endpoint Security and Control is an earlier iteration of the Intercept X & Central Endpoint Suite.</p> <div><h3>Intercept X & Central Endpoint Protection Overview</h3><p>Managed by Sophos Central</p><table><tr><th></th><th>SKU</th><th>CENTRAL ENDPOINT PROTECTION</th><th>INTERCEPT X ADVANCED</th><th>INTERCEPT X ADVANCED WITH EDR</th></tr><tr><td rowspan="21">PREVENT</td><td rowspan="5">ATTACK SURFACE REDUCTION</td><td>Web Security</td><td>✓</td><td>✓</td></tr><tr><td>Download Reputation</td><td>✓</td><td>✓</td></tr><tr><td>Web Control / Category-based URL Blocking</td><td>✓</td><td>✓</td></tr><tr><td>Peripheral Control (e.g. USB)</td><td>✓</td><td>✓</td></tr><tr><td>Application Control</td><td>✓</td><td>✓</td></tr><tr><td rowspan="5">BEFORE IT RUNS ON DEVICE</td><td>Deep Learning Malware Detection</td><td></td><td>✓</td><td>✓</td></tr><tr><td>Anti-Malware File Scanning</td><td>✓</td><td>✓</td><td>✓</td></tr><tr><td>Live Protection</td><td>✓</td><td>✓</td><td>✓</td></tr><tr><td>Pre-execution Behavior Analysis (HIPS)</td><td>✓</td><td>✓</td><td>✓</td></tr><tr><td>Potentially Unwanted Application (PUA) Blocking</td><td>✓</td><td>✓</td><td>✓</td></tr><tr><td rowspan="11">STOP RUNNING THREAT</td><td>Intrusion Prevention System (IPS, coming 2020)</td><td>✓</td><td>✓</td><td>✓</td></tr><tr><td>Data Loss Prevention</td><td>✓</td><td>✓</td><td>✓</td></tr><tr><td>Runtime Behavior Analysis (HIPS)</td><td>✓</td><td>✓</td><td>✓</td></tr><tr><td>Antimalware Scan Interface (AMSI)</td><td>✓</td><td>✓</td><td>✓</td></tr><tr><td>Malicious Traffic Detection (MTD)</td><td>✓</td><td>✓</td><td>✓</td></tr><tr><td>Exploit Prevention (details on page 2)</td><td></td><td>✓</td><td>✓</td></tr><tr><td>Active Adversary Mitigations (details on page 2)</td><td></td><td>✓</td><td>✓</td></tr><tr><td>Ransomware File Protection (CryptoGuard)</td><td></td><td>✓</td><td>✓</td></tr><tr><td>Disk and Boot Record Protection (WipeGuard)</td><td></td><td>✓</td><td>✓</td></tr><tr><td>Man-in-the-Browser Protection (Safe Browsing)</td><td></td><td>✓</td><td>✓</td></tr><tr><td>Enhanced Application Lockdown</td><td></td><td>✓</td><td>✓</td></tr><tr><td rowspan="5">DETECT AND INVESTIGATE</td><td rowspan="2">DETECT</td><td>Cross Estate Threat Searching (inc. files, scripts)</td><td></td><td>✓</td></tr><tr><td>Suspicious Events Detection and Prioritization</td><td></td><td>✓</td></tr><tr><td rowspan="3">INVESTIGATE</td><td>Threat Cases (Root Cause Analysis)</td><td></td><td>✓</td><td>✓</td></tr><tr><td>Deep Learning Malware Analysis</td><td></td><td></td><td>✓</td></tr><tr><td>Advanced On-demand SophosLabs Threat Intelligence</td><td></td><td></td><td>✓</td></tr><tr><td rowspan="5">RESPOND</td><td rowspan="5">REMEDiate</td><td>Forensic Data Export</td><td></td><td>✓</td></tr><tr><td>Automated Malware Removal</td><td>✓</td><td>✓</td><td>✓</td></tr><tr><td>Synchronized Security Heartbeat</td><td>✓</td><td>✓</td><td>✓</td></tr><tr><td>Sophos Clean</td><td></td><td>✓</td><td>✓</td></tr><tr><td>On-demand Endpoint Isolation</td><td></td><td></td><td>✓</td></tr><tr><td>Single-click "Clean and Block"</td><td></td><td></td><td>✓</td></tr></table></div>		SKU	CENTRAL ENDPOINT PROTECTION	INTERCEPT X ADVANCED	INTERCEPT X ADVANCED WITH EDR	PREVENT	ATTACK SURFACE REDUCTION	Web Security	✓	✓	Download Reputation	✓	✓	Web Control / Category-based URL Blocking	✓	✓	Peripheral Control (e.g. USB)	✓	✓	Application Control	✓	✓	BEFORE IT RUNS ON DEVICE	Deep Learning Malware Detection		✓	✓	Anti-Malware File Scanning	✓	✓	✓	Live Protection	✓	✓	✓	Pre-execution Behavior Analysis (HIPS)	✓	✓	✓	Potentially Unwanted Application (PUA) Blocking	✓	✓	✓	STOP RUNNING THREAT	Intrusion Prevention System (IPS, coming 2020)	✓	✓	✓	Data Loss Prevention	✓	✓	✓	Runtime Behavior Analysis (HIPS)	✓	✓	✓	Antimalware Scan Interface (AMSI)	✓	✓	✓	Malicious Traffic Detection (MTD)	✓	✓	✓	Exploit Prevention (details on page 2)		✓	✓	Active Adversary Mitigations (details on page 2)		✓	✓	Ransomware File Protection (CryptoGuard)		✓	✓	Disk and Boot Record Protection (WipeGuard)		✓	✓	Man-in-the-Browser Protection (Safe Browsing)		✓	✓	Enhanced Application Lockdown		✓	✓	DETECT AND INVESTIGATE	DETECT	Cross Estate Threat Searching (inc. files, scripts)		✓	Suspicious Events Detection and Prioritization		✓	INVESTIGATE	Threat Cases (Root Cause Analysis)		✓	✓	Deep Learning Malware Analysis			✓	Advanced On-demand SophosLabs Threat Intelligence			✓	RESPOND	REMEDiate	Forensic Data Export		✓	Automated Malware Removal	✓	✓	✓	Synchronized Security Heartbeat	✓	✓	✓	Sophos Clean		✓	✓	On-demand Endpoint Isolation			✓	Single-click "Clean and Block"			✓
	SKU	CENTRAL ENDPOINT PROTECTION	INTERCEPT X ADVANCED	INTERCEPT X ADVANCED WITH EDR																																																																																																																																			
PREVENT	ATTACK SURFACE REDUCTION	Web Security	✓	✓																																																																																																																																			
		Download Reputation	✓	✓																																																																																																																																			
		Web Control / Category-based URL Blocking	✓	✓																																																																																																																																			
		Peripheral Control (e.g. USB)	✓	✓																																																																																																																																			
		Application Control	✓	✓																																																																																																																																			
	BEFORE IT RUNS ON DEVICE	Deep Learning Malware Detection		✓	✓																																																																																																																																		
		Anti-Malware File Scanning	✓	✓	✓																																																																																																																																		
		Live Protection	✓	✓	✓																																																																																																																																		
		Pre-execution Behavior Analysis (HIPS)	✓	✓	✓																																																																																																																																		
		Potentially Unwanted Application (PUA) Blocking	✓	✓	✓																																																																																																																																		
	STOP RUNNING THREAT	Intrusion Prevention System (IPS, coming 2020)	✓	✓	✓																																																																																																																																		
		Data Loss Prevention	✓	✓	✓																																																																																																																																		
		Runtime Behavior Analysis (HIPS)	✓	✓	✓																																																																																																																																		
		Antimalware Scan Interface (AMSI)	✓	✓	✓																																																																																																																																		
		Malicious Traffic Detection (MTD)	✓	✓	✓																																																																																																																																		
		Exploit Prevention (details on page 2)		✓	✓																																																																																																																																		
		Active Adversary Mitigations (details on page 2)		✓	✓																																																																																																																																		
		Ransomware File Protection (CryptoGuard)		✓	✓																																																																																																																																		
		Disk and Boot Record Protection (WipeGuard)		✓	✓																																																																																																																																		
		Man-in-the-Browser Protection (Safe Browsing)		✓	✓																																																																																																																																		
		Enhanced Application Lockdown		✓	✓																																																																																																																																		
DETECT AND INVESTIGATE	DETECT	Cross Estate Threat Searching (inc. files, scripts)		✓																																																																																																																																			
		Suspicious Events Detection and Prioritization		✓																																																																																																																																			
	INVESTIGATE	Threat Cases (Root Cause Analysis)		✓	✓																																																																																																																																		
		Deep Learning Malware Analysis			✓																																																																																																																																		
		Advanced On-demand SophosLabs Threat Intelligence			✓																																																																																																																																		
RESPOND	REMEDiate	Forensic Data Export		✓																																																																																																																																			
		Automated Malware Removal	✓	✓	✓																																																																																																																																		
		Synchronized Security Heartbeat	✓	✓	✓																																																																																																																																		
		Sophos Clean		✓	✓																																																																																																																																		
		On-demand Endpoint Isolation			✓																																																																																																																																		
Single-click "Clean and Block"			✓																																																																																																																																				
	https://www.sophos.com/en-us/medialibrary/PDFs/factsheets/sophos-endpoint-license-guide.pdf																																																																																																																																						

Ex. D – Claim Chart
U.S. Patent No. 7,664,924

CLAIM 1	SOPHOS PRODUCTS																											
1[pre] In a computer comprising a storage medium and an application running on said computer, a method of controlling write access to said storage medium by said application comprising:	<div>This chart shows an overview of the Sophos Home versus Premium editions.</div> <table><tr><th></th><th>FREE</th><th>PREMIUM</th></tr><tr><td>Predictive Artificial Intelligence (AI) Threat Detection Identifies and blocks never-before-seen malware – including deep learning capabilities</td><td>✓</td><td>✓</td></tr><tr><td>Real-Time Antivirus Protects against known computer viruses, malware, Trojans, worms, bots, potentially unwanted apps (PUAs), ransomware, and more.</td><td>✓</td><td>✓</td></tr><tr><td>Parental Website Filtering Allows you to control the content your children can view online.</td><td>✓</td><td>✓</td></tr><tr><td>Web Protection Leverages the vast SophosLabs blacklist database to block compromised or dangerous websites.</td><td>✓</td><td>✓</td></tr><tr><td>Remote Management Secures multiple PCs and Macs in any location from a simple web interface.</td><td>✓</td><td>✓</td></tr><tr><td>Advanced Real-Time Threat Prevention Protects against new and developing viruses, malware, potentially unwanted apps (PUAs), and program exploits to prevent infection from the latest threats.</td><td>Expires after free 30-day trial of Sophos Home Premium</td><td>✓</td></tr><tr><td>Ransomware Security Stops the latest ransomware from encrypting your files and drives.</td><td>Expires after free 30-day trial of Sophos Home Premium</td><td>✓</td></tr><tr><td>Advanced Web Security Blocks phishing sites and bad or compromised websites for safe browsing and shopping.</td><td>Expires after free 30-day trial of Sophos Home Premium</td><td>✓</td></tr></table> <div>https://home.sophos.com/en-us/free-anti-virus-windows.aspx</div>		FREE	PREMIUM	Predictive Artificial Intelligence (AI) Threat Detection Identifies and blocks never-before-seen malware – including deep learning capabilities	✓	✓	Real-Time Antivirus Protects against known computer viruses, malware, Trojans, worms, bots, potentially unwanted apps (PUAs), ransomware, and more.	✓	✓	Parental Website Filtering Allows you to control the content your children can view online.	✓	✓	Web Protection Leverages the vast SophosLabs blacklist database to block compromised or dangerous websites.	✓	✓	Remote Management Secures multiple PCs and Macs in any location from a simple web interface.	✓	✓	Advanced Real-Time Threat Prevention Protects against new and developing viruses, malware, potentially unwanted apps (PUAs), and program exploits to prevent infection from the latest threats.	Expires after free 30-day trial of Sophos Home Premium	✓	Ransomware Security Stops the latest ransomware from encrypting your files and drives.	Expires after free 30-day trial of Sophos Home Premium	✓	Advanced Web Security Blocks phishing sites and bad or compromised websites for safe browsing and shopping.	Expires after free 30-day trial of Sophos Home Premium	✓
	FREE	PREMIUM																										
Predictive Artificial Intelligence (AI) Threat Detection Identifies and blocks never-before-seen malware – including deep learning capabilities	✓	✓																										
Real-Time Antivirus Protects against known computer viruses, malware, Trojans, worms, bots, potentially unwanted apps (PUAs), ransomware, and more.	✓	✓																										
Parental Website Filtering Allows you to control the content your children can view online.	✓	✓																										
Web Protection Leverages the vast SophosLabs blacklist database to block compromised or dangerous websites.	✓	✓																										
Remote Management Secures multiple PCs and Macs in any location from a simple web interface.	✓	✓																										
Advanced Real-Time Threat Prevention Protects against new and developing viruses, malware, potentially unwanted apps (PUAs), and program exploits to prevent infection from the latest threats.	Expires after free 30-day trial of Sophos Home Premium	✓																										
Ransomware Security Stops the latest ransomware from encrypting your files and drives.	Expires after free 30-day trial of Sophos Home Premium	✓																										
Advanced Web Security Blocks phishing sites and bad or compromised websites for safe browsing and shopping.	Expires after free 30-day trial of Sophos Home Premium	✓																										

Ex. D – Claim Chart
U.S. Patent No. 7,664,924

CLAIM 1	SOPHOS PRODUCTS
<p>1[pre] In a computer comprising a storage medium and an application running on said computer, a method of controlling write access to said storage medium by said application comprising:</p>	<p>Sophos's software operates and runs on a computer such as a PC, Mac, or Server with a storage medium such as a hard disk or memory. The software controls write access to the computer's storage medium to prevent malicious files from being written to the device, which is a central purpose of the software sold by Sophos. As shown below, Sophos's software analyzes applications running on the computer and blocks activity of the applications that appear to be malicious, including blocking write access.</p> <div data-bbox="669 626 1736 1005" style="border: 1px solid black; padding: 10px; margin: 10px 0;"> <p>Malicious and suspicious behavior detection</p> <p>Suspicious behavior detection uses Sophos's Host Intrusion Prevention System (HIPS) to dynamically analyze the behavior of all programs running on the computer to detect and block activity that appears to be malicious. Suspicious behavior may include changes to the registry that could allow a virus to run automatically when the computer is restarted.</p> <p>Suspicious behavior detection watches all system processes for signs of active malware, such as suspicious writes to the registry or file copy actions. It can be set to warn the administrator and/or block the process.</p> <p>Malicious behavior detection dynamically analyses all programs running on the computer to detect and block activity that is known to be malicious.</p> </div> <p>https://docs.sophos.com/esg/endpoint-security-and-control/10-6/help/en-us/PDF/sesc_h.pdf at 25-26.</p>

Ex. D – Claim Chart
U.S. Patent No. 7,664,924

CLAIM 1	SOPHOS PRODUCTS
1[a] detecting an attempt by the application to write data to said storage medium;	<p>Sophos’s software detects attempts by the application to write data to said storage medium. For example, Sophos’s “malicious behavior detection” analyses programs running on the computer to detect and block known malicious activity, including attempts to write data to the storage medium. As shown below, using Sophos’s Behavior Monitoring, Sophos’s “suspicious behavior detection” analyzes the behavior of program and watches for signs of malware, such as suspicious writes to the registry or file copy actions.”</p> <div data-bbox="669 626 1736 1005" style="border: 1px solid black; padding: 10px; margin: 10px 0;"> <p>Malicious and suspicious behavior detection</p> <p>Suspicious behavior detection uses Sophos’s Host Intrusion Prevention System (HIPS) to dynamically analyze the behavior of all programs running on the computer to detect and block activity that appears to be malicious. Suspicious behavior may include changes to the registry that could allow a virus to run automatically when the computer is restarted.</p> <p>Suspicious behavior detection watches all system processes for signs of active malware, such as suspicious writes to the registry or file copy actions. It can be set to warn the administrator and/or block the process.</p> <p>Malicious behavior detection dynamically analyses all programs running on the computer to detect and block activity that is known to be malicious.</p> </div> <p>https://docs.sophos.com/esg/endpoint-security-and-control/10-6/help/en-us/PDF/sesc_h.pdf at 25-26.</p>

Ex. D – Claim Chart
U.S. Patent No. 7,664,924

CLAIM 1	SOPHOS PRODUCTS								
<p>1[a] detecting an attempt by the application to write data to said storage medium;</p>	<p>As another example, Sophos’s “on-access scanning,” detects attempts by the application to write data to said storage medium. For example, on-access scanning detects any attempts to open, save, copy or rename a file, which necessarily includes an attempt by the application to write data to said storage medium. Further, “on-access scanning” may be set to “check files on write.”</p> <div data-bbox="615 545 1785 834" style="border: 1px solid black; padding: 10px; margin: 10px 0;"> <p>On-access scanning</p> <p>On-access scanning is your main method of protection against viruses and other threats.</p> <p>Whenever you open, save, copy or rename a file, Sophos Anti-Virus scans the file and grants access to it only if it does not pose a threat to your computer or has been authorized for use.</p> <p>For more information, see Configure on-access scanning (page 7).</p> </div> <div data-bbox="615 922 1822 1224" style="border: 1px solid black; padding: 10px; margin: 10px 0;"> <p>2. To change when on-access scanning occurs, under Check files on, set the options as described below.</p> <table border="1" data-bbox="669 1023 1814 1214"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td>Read</td><td>Scan files when they are copied, moved, or opened.</td></tr> <tr> <td>Rename</td><td>Scan files when they are renamed.</td></tr> <tr> <td>Write</td><td>Scan files when they are saved or created.</td></tr> </tbody> </table> </div> <p>https://docs.sophos.com/esg/endpoint-security-and-control/10-6/help/en-us/PDF/sesc_h.pdf at 7-8.</p>	Option	Description	Read	Scan files when they are copied, moved, or opened.	Rename	Scan files when they are renamed.	Write	Scan files when they are saved or created.
Option	Description								
Read	Scan files when they are copied, moved, or opened.								
Rename	Scan files when they are renamed.								
Write	Scan files when they are saved or created.								

Ex. D – Claim Chart
U.S. Patent No. 7,664,924

CLAIM 1	SOPHOS PRODUCTS		
<p>1[b] in response to said write attempt, attempting to retrieve a permission value from a database comprised of data elements encoding at least one permission value associated with one or more applications;</p>	<p>In response to the write attempts discussed for limitation 1[a], the Sophos software attempts to retrieve a permission value from a database comprised of data elements encoding at least one permission value associated with one or more applications. For example, the Sophos software utilizes rules, policies, whitelists, authorized lists, and/or exceptions that are stored in a database. For example, Sophos’s “Authorized list” includes at least one permission value (e.g., an authorization) associated with each item on the list, and each item is associated with an application.</p> <div data-bbox="646 643 1812 850"> <table border="1"> <tr> <td data-bbox="653 647 1230 846">Authorize</td><td data-bbox="1230 647 1806 846"> <p>Users can authorize suspicious items, adware, and PUAs in order to allow them to run on the computer.</p> <p>This option applies to both Authorization manager and Quarantine manager.</p> </td></tr> </table> </div> <div data-bbox="646 902 1812 1218"> <p>If you want to allow an item that Sophos Anti-Virus has classified as suspicious, you can authorize it as follows.</p> <ol style="list-style-type: none"> 1. Click Home > Anti-virus and HIPS > Configure anti-virus and HIPS > Configure > Authorization. 2. Click the tab for the type of item that has been detected (for example, Buffer overflow). 3. In the Known list, select the suspicious item. 4. Click Add. <p>The suspicious item appears in the Authorized list.</p> </div> <p>https://docs.sophos.com/esg/endpoint-security-and-control/10-6/help/en-us/PDF/sesc_h.pdf at 6, 32.</p>	Authorize	<p>Users can authorize suspicious items, adware, and PUAs in order to allow them to run on the computer.</p> <p>This option applies to both Authorization manager and Quarantine manager.</p>
Authorize	<p>Users can authorize suspicious items, adware, and PUAs in order to allow them to run on the computer.</p> <p>This option applies to both Authorization manager and Quarantine manager.</p>		

Ex. D – Claim Chart
U.S. Patent No. 7,664,924

CLAIM 1	SOPHOS PRODUCTS
<p>1[b] in response to said write attempt, attempting to retrieve a permission value from a database comprised of data elements encoding at least one permission value associated with one or more applications;</p>	<p>As another example, Sophos’s software includes “whitelists.” Sophos’s “whitelist” includes at lease one permission value (e.g., an authorization) associated with each item on the list, and each item is associated with an application.</p> <div data-bbox="573 630 1833 993" style="border: 1px solid black; padding: 10px; margin: 10px 0;"> <p>Further information</p> <p>Given the number of files scanned by Sophos Anti-Virus a look-up can be triggered quite frequently. This is not an event that an end user would see but you may see traffic if monitoring your firewall etc.</p> <p>To limit the number of look-ups SophosLabs also whitelists common files, so they will not be scanned, this includes OS files but also common applications. Due to the nature of malware we attempt to reduce the number of look-ups where possible but do not set an arbitrary limit as we do not want to compromise on the protection we offer customers and the rapid response cloud look-ups.</p> </div> <p>https://community.sophos.com/kb/en-us/111334</p>

Ex. D – Claim Chart
U.S. Patent No. 7,664,924

CLAIM 1	SOPHOS PRODUCTS
<p>1[b] in response to said write attempt, attempting to retrieve a permission value from a database comprised of data elements encoding at least one permission value associated with one or more applications;</p>	<p>In yet another example, Sophos’s software includes an allow list. Sophos’s “allow list” includes at least one permission value (e.g., an authorization) associated with each item on the list, and each item is associated with an application. The items on list are stored on a database that include data elements encoding permission values, e.g., “authorized,” that are associated with the items on the list. While an allow list is maintained by SophosLabs, the list is provided to and stored in the computer to “improve performance.”</p> <div data-bbox="588 568 1854 889" style="border: 1px solid black; padding: 10px; margin: 10px 0;"> <p>How does it work?</p> <p>LiveProtection will perform a lookup for any file it suspects of being malware; the following events will trigger a lookup</p> <ul style="list-style-type: none"> • Whenever a file is added to the endpoint’s quarantine manager. • Whenever reported internally by the anti-malware engine that a file is deemed suitably suspicious. • Whenever reported internally by anti-malware engine that a file is to be checked against a allow list defined by SophosLabs. (The allow list is maintained by SophosLabs and contains a list of common and system files which the product should cache to improve performance.) </div> <p>https://community.sophos.com/kb/en-us/110921</p>

Ex. D – Claim Chart
U.S. Patent No. 7,664,924

CLAIM 1	SOPHOS PRODUCTS
<p>1[b] in response to said write attempt, attempting to retrieve a permission value from a database comprised of data elements encoding at least one permission value associated with one or more applications;</p>	<p>In yet another example, Sophos's software may exclude certain files, folder, and/or drives from on-access scanning. The information regarding the excluded files, folders, and/or drives are store on a database that include data elements encoding permission values, e.g., specifying not to scan. The values are associated with one or more applications (e.g., the applications within the files, folder, and/or drives).</p> <div data-bbox="667 565 1717 1159" style="border: 1px solid black; padding: 10px; margin: 10px 0;"> <p>5.4.1 Exclude items from on-access scanning</p> <p>Important If a management console is used to administer Sophos Endpoint Security and Control on this computer, it may override any changes you make here.</p> <p>To edit the list of files, folders, and drives that are excluded from on-access scanning:</p> <ol style="list-style-type: none"> 1. Click Home > Anti-virus and HIPS > Configure anti-virus and HIPS > Configure > On-access scanning. 2. Click the Exclusions tab, and then choose one of the following options. <ul style="list-style-type: none"> • To specify a file, folder, or drive that should be excluded from on-access scanning, click Add. • To delete an exclusion, click Remove. • To change an exclusion, click Edit. 3. To add or edit an excluded item, in the Exclude item dialog box, select the Item type. The All remote files item type is for excluding files that are not stored on local drives. You might select this if you want to increase speed of access to such files and you trust the available remote file locations. 4. Specify the Item name by using the Browse button or typing in the text box. </div> <p>https://docs.sophos.com/esg/endpoint-security-and-control/10-6/help/en-us/PDF/sesc_h.pdf at 21</p>

Ex. D – Claim Chart
U.S. Patent No. 7,664,924

CLAIM 1	SOPHOS PRODUCTS
<p>1[b] in response to said write attempt, attempting to retrieve a permission value from a database comprised of data elements encoding at least one permission value associated with one or more applications;</p>	<p>Similarly, Sophos's software may exclude certain file types from on-access scanning. The information regarding the file types are stored on a database that include data elements encoding permission values, e.g., specifying files types to scan. The values are associated with one or more applications (e.g., by file extension type).</p> <div data-bbox="575 492 1675 1089" style="border: 1px solid black; padding: 10px; margin: 10px 0;"> <p>5.2.6 Specify on-access scanning file extensions</p> <p>Important If a management console is used to administer Sophos Endpoint Security and Control on this computer, it may override any changes you make here.</p> <p>You can specify which file extensions are scanned during on-access scanning.</p> <ol style="list-style-type: none"> 1. Click Home > Anti-virus and HIPS > Configure anti-virus and HIPS > Configure > On-access scanning. 2. Click the Extensions tab, set the options as described below. <p>Scan all files Click this to enable scanning of all files, regardless of the filename extension.</p> <p>Allow me to control exactly what is scanned Click this to restrict scanning to only files with a particular filename extension, specified in the extension list.</p> </div> <p>https://docs.sophos.com/esg/endpoint-security-and-control/10-6/help/en-us/PDF/sesc_h.pdf at 11</p>

Ex. D – Claim Chart
U.S. Patent No. 7,664,924

CLAIM 1	SOPHOS PRODUCTS
<p>1[b] in response to said write attempt, attempting to retrieve a permission value from a database comprised of data elements encoding at least one permission value associated with one or more applications;</p>	<p>As yet another example, Sophos’s software causes “threat identity (IDE)” files to be stored on a database in the computer. The IDE files include a permission value indicating whether the item is malicious. The database is comprised of data elements encoding at least one permission value (malicious or not) associated with the one or more applications.</p> <div data-bbox="640 597 1749 1221" style="border: 1px solid black; padding: 10px; margin: 10px 0;"> <p>Sophos Live Protection - What is it?</p> <p>As malware continues to rapidly evolve and grow, Sophos has realized that it needs a way to enhance existing data updates with a system to keep endpoint protection up to date in real-time. This was done to both improve the response time to new malware and reduce the amount of data delivered to the endpoints.</p> <p>LiveProtection was added to give the endpoint the ability to 'lookup' files in real-time to verify if they are malicious. Over the past few years it has proven very effective at stopping new malware outbreaks and protecting our customers.</p> <p>Sophos Live Protection can perform the following tasks:</p> <ul style="list-style-type: none"> • Perform cloud look-ups against individual files to determine if safe/malicious <p>If the anti-virus scan on an endpoint computer has identified a file as suspicious, but cannot further identify it as either clean or malicious based on the threat identity (IDE) files stored on the computer, certain file data (such as its checksum and other attributes) is sent to Sophos to assist with further analysis. This is known as 'in-the-cloud' checking: it performs an instant lookup of a suspicious file in the SophosLabs database. If the file is identified as clean or malicious, the decision is sent back to the computer and the status of the file is automatically updated.</p> </div> <p>https://community.sophos.com/kb/en-us/110921</p>

Ex. D – Claim Chart
U.S. Patent No. 7,664,924

CLAIM 1	SOPHOS PRODUCTS
<p>1[c] in the case that no permission value for the running application is found in the database, transmitting to a central server operatively connected to the computer and to at least one additional computer, a query comprised of an indicia of identity associated with said running application;</p>	<p>In the case where no permission value for the running application is found in the database (e.g., the application is not authorized, whitelisted, allowed, excluded or present on an IDE file) the Sophos software transmits a query (e.g., a “DNS query”) comprised of an indicia of identity associated with said running application (e.g., “certain file data”) to a central server operatively connected to the computer and to at least one additional computer. (e.g., Sophos’s SophosLabs server). For example, this step occurs via “live lookups” to “check suspicious files.”</p> <div data-bbox="648 727 1732 995" style="border: 1px solid black; padding: 10px; margin: 20px 0;"> <p>• Enable Live Protection</p> <p>If the anti-virus scan on an endpoint computer has identified a file as suspicious, but cannot further identify it as either clean or malicious based on the threat identity (IDE) files stored on the computer, certain file data (such as its checksum and other attributes) is sent to Sophos to assist with further analysis.</p> <p>The in-the-cloud checking performs an instant lookup of a suspicious file in the SophosLabs database. If the file is identified as clean or malicious, the decision is sent back to the computer and the status of the file is automatically updated.</p> </div> <p>https://docs.sophos.com/esg/endpoint-security-and-control/10-6/help/en-us/PDF/sesc_h.pdf at 28</p>

Ex. D – Claim Chart
U.S. Patent No. 7,664,924

CLAIM 1	SOPHOS PRODUCTS
<p>1[c] in the case that no permission value for the running application is found in the database, transmitting to a central server operatively connected to the computer and to at least one additional computer, a query comprised of an indicia of identity associated with said running application;</p>	<p>As an example, the software “Automatically trigger[s] live lookups to SophosLabs to check suspicious files.”</p> <div data-bbox="674 483 1694 1065" style="border: 1px solid black; padding: 10px; margin: 10px 0;"> <p>Anti-virus and HIPS policies – virus, spyware, PUA, intrusion prevention</p> <p>Implementing our anti-virus protection also provides you with a complete host intrusion prevention system (HIPS) and in-the-cloud real time protection without the need for complex installation and configuration. It enables you to quickly and easily implement a range of protection technologies - unique pre-execution scanning, runtime analysis, buffer overflow and live protection - that all combine to proactively detect malware and suspicious files and behavior. The policy</p> <p>lets you specify scanning requirements for on-access, on-demand, scheduled, and web scanning and you can opt to exclude particular file types where they are known to pose no threat. By default, computers will use the following standard policy:</p> <ul style="list-style-type: none"> • Scan all files that are vulnerable to malware. • Deny access to any file that contains a virus, spyware, etc. • Display an alert on the desktop of any computer where a virus or PUA is found. • Automatically trigger live lookups to SophosLabs to check suspicious files </div> <p>https://www.sophos.com/en-us/medialibrary/pdfs/factsheets/sophosendpointsecurityanddataprotectionrgna.pdf at 14</p>

Ex. D – Claim Chart
U.S. Patent No. 7,664,924

CLAIM 1	SOPHOS PRODUCTS
<p>1[c] in the case that no permission value for the running application is found in the database, transmitting to a central server operatively connected to the computer and to at least one additional computer, a query comprised of an indicia of identity associated with said running application;</p>	<p>More specifically, the “endpoint” (i.e., the computer) can perform cloud look-ups against individual files to determine if safe/malicious. This lookup (i.e., query) will necessarily comprise an indicia of identity associated with said running application for SophosLabs to “lookup” the application in the database.</p> <div data-bbox="625 558 1736 1180" style="border: 1px solid black; padding: 10px; margin: 10px 0;"> <p>Sophos Live Protection - What is it?</p> <p>As malware continues to rapidly evolve and grow, Sophos has realized that it needs a way to enhance existing data updates with a system to keep endpoint protection up to date in real-time. This was done to both improve the response time to new malware and reduce the amount of data delivered to the endpoints.</p> <p>LiveProtection was added to give the endpoint the ability to 'lookup' files in real-time to verify if they are malicious. Over the past few years it has proven very effective at stopping new malware outbreaks and protecting our customers.</p> <p>Sophos Live Protection can perform the following tasks:</p> <ul style="list-style-type: none"> • Perform cloud look-ups against individual files to determine if safe/malicious <p>If the anti-virus scan on an endpoint computer has identified a file as suspicious, but cannot further identify it as either clean or malicious based on the threat identity (IDE) files stored on the computer, certain file data (such as its checksum and other attributes) is sent to Sophos to assist with further analysis. This is known as 'in-the-cloud' checking: it performs an instant lookup of a suspicious file in the SophosLabs database. If the file is identified as clean or malicious, the decision is sent back to the computer and the status of the file is automatically updated.</p> </div> <p>https://community.sophos.com/kb/en-us/110921</p>

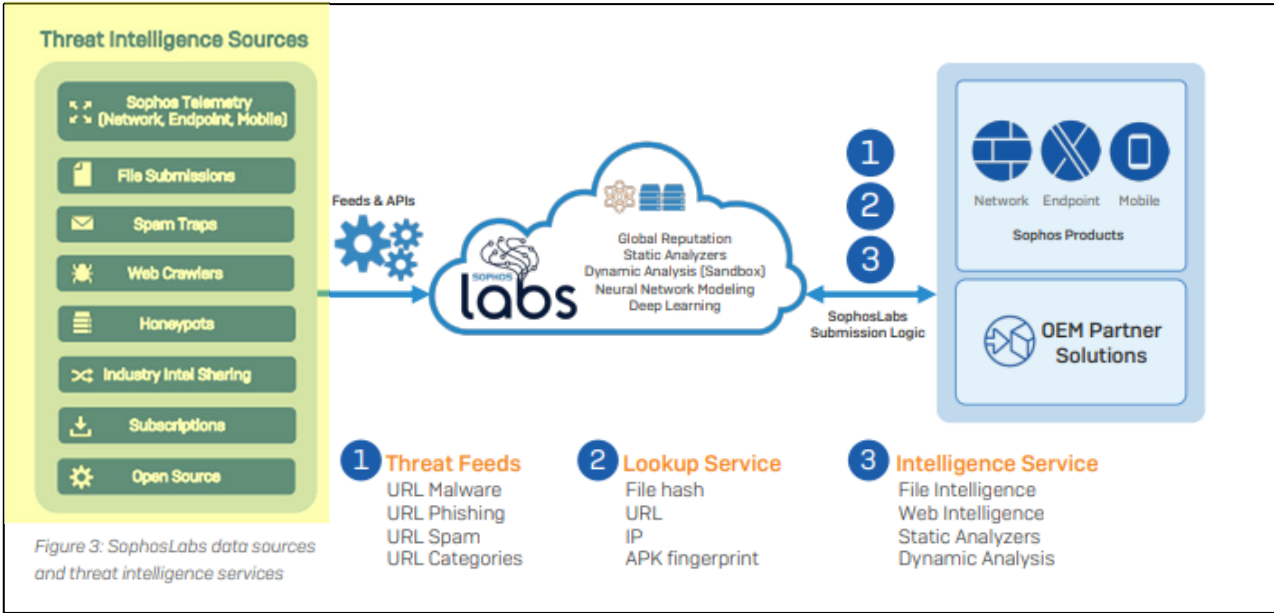
Ex. D – Claim Chart
U.S. Patent No. 7,664,924

CLAIM 1	SOPHOS PRODUCTS
<p>1[c] in the case that no permission value for the running application is found in the database, transmitting to a central server operatively connected to the computer and to at least one additional computer, a query comprised of an indicia of identity associated with said running application;</p>	<p>Sophos's software on the endpoint performs the lookups over DNS queries as shown below.</p> <div data-bbox="583 435 1646 834" style="border: 1px solid black; padding: 10px; margin: 10px 0;"> <p>Lookups - further information</p> <p>LiveProtection performs a lookup to ensure the most up to date protection as new information could have been discovered about the file since the last time it was scanned.</p> <p>Lookups contain a limited amount of information and are designed to help SophosLabs analysts to package up specific malware related information (such as function bytes or other properties required) to increase accuracy of detections.</p> <p>Lookups are performed over DNS and the average endpoint perform a large number lookups per day depending on the level of activity. During scheduled and on-demand scans the number will increase as all files on the system will be accessed which triggers an increased number of lookups compared to normal operations.</p> </div> <p>https://community.sophos.com/kb/en-us/110921</p> <div data-bbox="583 922 1677 1305" style="border: 1px solid black; padding: 10px; margin: 10px 0;"> <p>How does it work</p> <p>In some IDEs, SophosLabs include special instructions to trigger a live lookup for more up-to-date threat information. When one of the lookup-enabled identities is triggered, generic information about the threat and the detection is sent to SophosLabs using SXL, a protocol/framework designed and maintained by Sophos that runs over DNS queries. If new information is available the endpoint receives it in the SXL response and adjusts its behavior accordingly. Also, if based on the lookup information, SophosLabs deem the file interesting for further research the endpoint automatically uploads the sample.</p> <p>When a lookup-enabled detection is triggered by the on-access scanner, on-demand scanner, or runtime HIPS, the SAV service performs a specially crafted DNS query that includes generic information about the file and the detection features, to the sophosxl.net name servers. It then takes action(s) based on the response it gets.</p> </div> <p>https://community.sophos.com/kb/en-us/111334</p>

Ex. D – Claim Chart
U.S. Patent No. 7,664,924

CLAIM 1	SOPHOS PRODUCTS
<p>1[c] in the case that no permission value for the running application is found in the database, transmitting to a central server operatively connected to the computer and to at least one additional computer, a query comprised of an indicia of identity associated with said running application;</p>	<p>The SophosLabs server is connected to at least one additional computer. For example, each endpoint with Sophos's Live Protection technology is operatively connected to the SophosLabs server. As another example, additional computers are associated with Sophos's agents who analyze malware and provide updates to the server based on the analysis.</p> <div data-bbox="575 518 1629 695" style="border: 1px solid black; padding: 10px; margin: 10px 0;"> <p>SophosLabs keeps a round-the-clock watch on new threats, with experts analyzing new malware across every time zone and delivering the fastest, smallest updates.</p> </div> <p>https://www.sophos.com/en-us/medialibrary/pdfs/factsheets/sophosendpointsecurityanddataprotectionrgna.pdf at 14</p>

Ex. D – Claim Chart
U.S. Patent No. 7,664,924

CLAIM 1	SOPHOS PRODUCTS
<p>1[c] in the case that no permission value for the running application is found in the database, transmitting to a central server operatively connected to the computer and to at least one additional computer, a query comprised of an indicia of identity associated with said running application;</p>	<p>The server is connected to numerous additional computers, as shown below.</p>  <p><i>Figure 3: SophosLabs data sources and threat intelligence services</i></p>

<https://www.sophos.com/en-us/medialibrary/pdfs/factsheets/oem-solutions/sophos-threat-intelligence-dsna.pdf> at 3

Ex. D – Claim Chart
U.S. Patent No. 7,664,924

CLAIM 1	SOPHOS PRODUCTS
<p>1[d] receiving from said central server, data that represents the collective response of the user of the at least one additional computer to requests by the same application running on said at least one additional computer to access the storage medium that comprises said at least one additional computer.</p>	<p>The Sophos software causes the computer to receive from said central server, data that represents the collective response of the user of the at least one additional computer to requests by the same application running on said at least one additional computer to access the storage medium that comprises said at least one additional computer. For example, the computer receives a response from the server that includes data indicating the status of the file.</p> <div data-bbox="577 586 1661 854" style="border: 1px solid black; padding: 10px;"> <p>• Enable Live Protection</p> <p>If the anti-virus scan on an endpoint computer has identified a file as suspicious, but cannot further identify it as either clean or malicious based on the threat identity (IDE) files stored on the computer, certain file data (such as its checksum and other attributes) is sent to Sophos to assist with further analysis.</p> <p>The in-the-cloud checking performs an instant lookup of a suspicious file in the SophosLabs database. If the file is identified as clean or malicious, the decision is sent back to the computer and the status of the file is automatically updated.</p> </div> <p>https://docs.sophos.com/esg/endpoint-security-and-control/10-6/help/en-us/PDF/sesc_h.pdf at 28</p>

Ex. D – Claim Chart
U.S. Patent No. 7,664,924

CLAIM 1	SOPHOS PRODUCTS
<p>1[d] receiving from said central server, data that represents the collective response of the user of the at least one additional computer to requests by the same application running on said at least one additional computer to access the storage medium that comprises said at least one additional computer.</p>	<p>As another example, the computer receives a response from the server that includes data indicating an action to take.</p> <div data-bbox="579 435 1829 977" style="border: 1px solid black; padding: 10px;"> <p>How does it work</p> <p>In some IDEs, SophosLabs include special instructions to trigger a live lookup for more up-to-date threat information. When one of the lookup-enabled identities is triggered, generic information about the threat and the detection is sent to SophosLabs using SXL, a protocol/framework designed and maintained by Sophos that runs over DNS queries. If new information is available the endpoint receives it in the SXL response and adjusts its behavior accordingly. Also, if based on the lookup information, SophosLabs deem the file interesting for further research the endpoint automatically uploads the sample.</p> <p>When a lookup-enabled detection is triggered by the on-access scanner, on-demand scanner, or runtime HIPS, the SAV service performs a specially crafted DNS query that includes generic information about the file and the detection features, to the sophosxl.net name servers. It then takes action(s) based on the response it gets.</p> <p>Currently available actions include:</p> <ul style="list-style-type: none"> • Ignore the detection, for instance if the file is known to be detected as a false positive • Treat the detection as malware • Treat the detection as suspicious • Request a sample (performed only if allowed by the policy and, please note, only applies to executable files) </div> <p>https://community.sophos.com/kb/en-us/111334</p>

Ex. D – Claim Chart
U.S. Patent No. 7,664,924

CLAIM 1	SOPHOS PRODUCTS
<p>1[d] receiving from said central server, data that represents the collective response of the user of the at least one additional computer to requests by the same application running on said at least one additional computer to access the storage medium that comprises said at least one additional computer.</p>	<p>The data in the response mentioned previously represents the collective response of the user of the at least one additional computer. The data is based on the “aggregating telemetry” of the additional computers operatively connected to the server.</p> <div data-bbox="573 475 1709 1206"> <p>Data Sources and Curation It all starts with aggregating telemetry from Sophos network, endpoint and mobile products with a variety of complementary data sources to gain global visibility. Our automated curation deduplicates entries, categorizes threat objects, reduces false positives and updates reputations. Conflicting threat data is escalated for review by our threat experts.</p> <p style="font-size: small;">Figure 3: SophosLabs data sources and threat intelligence services</p> </div> <p>https://www.sophos.com/en-us/medialibrary/pdfs/factsheets/oem-solutions/sophos-threat-intelligence-dsna.pdf at 3</p>

Ex. D – Claim Chart
U.S. Patent No. 7,664,924

CLAIM 1	SOPHOS PRODUCTS
<p>1[d] receiving from said central server, data that represents the collective response of the user of the at least one additional computer to requests by the same application running on said at least one additional computer to access the storage medium that comprises said at least one additional computer.</p>	<p>Moreover, Sophos's agents (i.e., its experts) review threat information using an additional computer operatively coupled to the server. The expert's response via the additional computer is stored in the server and is represented by the data in the response that is sent to the computer.</p> <div data-bbox="697 519 1719 1183" data-label="Diagram"> <p>Data Sources and Curation It all starts with aggregating telemetry from Sophos network, endpoint and mobile products with a variety of complementary data sources to gain global visibility. Our automated curation deduplicates entries, categorizes threat objects, reduces false positives and updates reputations. Conflicting threat data is escalated for review by our threat experts.</p> <p>Threat Intelligence Sources</p> <ul style="list-style-type: none"> Sophos Telemetry (Network, Endpoint, Mobile) File Submissions Spam Traps Web Crawlers Honeypots Industry Intel Sharing Subscriptions Open Source <p>Feeds & APIs → Sophos Labs (Global Reputation, Static Analyzers, Dynamic Analysis [Sandbox], Neural Network Modeling, Deep Learning)</p> <p>1 Threat Feeds URL Malware URL Phishing URL Spam URL Categories</p> <p>2 Lookup Service File hash URL IP APK fingerprint</p> <p>3 Intelligence Service File Intelligence Web Intelligence Static Analyzers Dynamic Analysis</p> <p>Sophos Labs Submission Logic → Sophos Products (Network, Endpoint, Mobile) and OEM Partner Solutions</p> <p><i>Figure 3: SophosLabs data sources and threat intelligence services</i></p> </div> <p>https://www.sophos.com/en-us/medialibrary/pdfs/factsheets/oem-solutions/sophos-threat-intelligence-dsna.pdf at 3</p>

Ex. D – Claim Chart
U.S. Patent No. 7,664,924

CLAIM 1	SOPHOS PRODUCTS
<p>1[d] receiving from said central server, data that represents the collective response of the user of the at least one additional computer to requests by the same application running on said at least one additional computer to access the storage medium that comprises said at least one additional computer.</p>	<p>The data in the response, mentioned in the last slide represents the collective response of the user of the at least one additional computer. For example, Sophos's agents (its experts) use an additional computer to provide responses.</p> <div data-bbox="577 483 1633 657" style="border: 1px solid black; padding: 10px; margin: 10px 0;"> <p>SophosLabs keeps a round-the-clock watch on new threats, with experts analyzing new malware across every time zone and delivering the fastest, smallest updates.</p> </div> <p>https://www.sophos.com/en-us/medialibrary/pdfs/factsheets/sophosendpointsecurityanddataprotectionrgna.pdf at 14</p>

Ex. D – Claim Chart
U.S. Patent No. 7,664,924

CLAIM 1	SOPHOS PRODUCTS						
1[d] receiving from said central server, data that represents the collective response of the user of the at least one additional computer to requests by the same application running on said at least one additional computer to access the storage medium that comprises said at least one additional computer.	<p>As another example, Sophos uses additional computers for its sandbox. During review of files in the sandbox, a user of the additional computer provides a response related to the file. The central server provides the collective response to the endpoint.</p> <div><p>Dynamic Analysis (Cloud Sandbox)</p><p>SophosLabs Cloud Sandbox utilizes the latest analysis techniques to identify malicious files for unmatched visibility into unknown files.</p><p>Key Features</p><table><thead><tr><th>Malware and Potentially Unwanted Apps (PUA) detections</th><th>Known Malware Families</th><th>Other Malicious Behaviors</th></tr></thead><tbody><tr><td><ul style="list-style-type: none">› Sophos antivirus file and memory detections› Sophos Intercept X machine learning, CryptoGuard, and WipeGuard technologies</td><td><ul style="list-style-type: none">› Yara patterns deep memory scans› Behavior patterns – IOCs attributed to malware</td><td><ul style="list-style-type: none">› Evasion – anti-sandbox and anti-virtual machine tactics› Cryptomining› Deception technology</td></tr></tbody></table></div> <p>https://www.sophos.com/en-us/medialibrary/pdfs/factsheets/oem-solutions/sophos-threat-intelligence-dsna.pdf at 6</p>	Malware and Potentially Unwanted Apps (PUA) detections	Known Malware Families	Other Malicious Behaviors	<ul style="list-style-type: none">› Sophos antivirus file and memory detections› Sophos Intercept X machine learning, CryptoGuard, and WipeGuard technologies	<ul style="list-style-type: none">› Yara patterns deep memory scans› Behavior patterns – IOCs attributed to malware	<ul style="list-style-type: none">› Evasion – anti-sandbox and anti-virtual machine tactics› Cryptomining› Deception technology
Malware and Potentially Unwanted Apps (PUA) detections	Known Malware Families	Other Malicious Behaviors					
<ul style="list-style-type: none">› Sophos antivirus file and memory detections› Sophos Intercept X machine learning, CryptoGuard, and WipeGuard technologies	<ul style="list-style-type: none">› Yara patterns deep memory scans› Behavior patterns – IOCs attributed to malware	<ul style="list-style-type: none">› Evasion – anti-sandbox and anti-virtual machine tactics› Cryptomining› Deception technology					